

Comments From CellSafe LLC

CellSafe LLC., hereby submits its comments in response to the Notice of Proposed Rulemaking titled “Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities, GN Docket No. 13-111”.

Introduction

CellSafe LLC. is a small veteran owned business with 7 years of experience developing and deploying cell phone detection/location systems for classified customers and correctional facilities. The product has a deployed footprint around the world in a variety of applications with thousands of sensors monitoring cellular activity for our customers on a continuous basis.

Comments

Having the FCC involved in the investigation of various technical solutions to combat the use of contraband wireless devices in correctional facilities is an essential step in finding a workable solution. Numerous government Agencies, State and Federal, launched similar efforts over the past 6 years, but the studies never were followed with a comprehensive test plan to rigorously test and evaluate proposed solutions. Those tests conducted were more like show and tell events delaying the implementation of a satisfactory solution for corrections. Streamlining an approval process for spectral use may be helpful in addressing the contraband cell phone issue. That is provided the system solutions proposed do not have more negative unintended consequences than the problem they are designed to address.

The problem, at its very root, is not just contraband cell phones, but unmonitored communications of all forms. Several high profile incidents involving contraband cell phones spawned a lot of news in the press raising public awareness and ire over the problem.

A theory held by some in the corrections industry is contraband phones can be jammed or denied service by some scheme resolving the problem and security resolved. In the security world there is something worse than no security and that is a false sense of security. Cell phone jamming or redirection may provide a level of protection in facilities in remote locations and a frustration level for inmates unable to use their phones, but it is not by any measure a complete solution to the security threat created by unmonitored cell phone based communications.

There is a difference of opinion on how one might mitigate the problem of contraband cell phones between correctional administration and the security staff responsible. Correctional Administration staff generally has taken the position that preventing cell phones from communicating to the carrier

networks by any means rendering the device incapable of communicating over the RF link. Leading one state corrections secretary to espouse, “We will turn their phones into paperweights”. While this approach might have been true 10 or more years ago when a phones only utility was to talk to the carrier network, it is clearly not true today. This attitude or response to the problem only serves to minimize the issue, simplify the problem, and create a whole new set of problems which need to be addressed.

Security staffs understand operating a safe and secure facility means keeping your finger on the pulse of the inmate leaders, trouble makers, gangs, and potential hot spots. This is done by collecting information in and from various sources while stitching all of the inputs together to paint a potential threat picture. This approach is no different than a US Government intelligence agencies methodology when it comes to terrorism threats. The option to deny cellular service to a terrorist by jamming or denial of service techniques might disrupt the threat in the short term, but not eliminate the threat. When a threat picture has been created with high certainty of an impending event this is the optimum time to deny service or jam. You need the intelligence to make an informed decision on how best to thwart an action, maximizing the effect of the intervention.

As a proponent for cellular detection systems, several arguments or points substantiate this position.

First, detection systems do not transmit any RF and therefore obviate the need for agreements between the technology and telecom providers and concurrently not interfere with other communications devices or services.

Secondly, the one sure way to eliminate all threats from a contraband cell phone is to find and remove the handset rendering SIM and Memory of no value. Finding the handset requires a system with sufficient fidelity to minimize the search area. Detection systems used in conjunction with other available technology products such as non-linear junction wands and cell phone sniffing dogs can further assist in reducing search times and manpower.

Thirdly, when one determines the location of a cell phone, the location generally reveals not only the active users, but many times have proven to be the location of other contraband. Jamming and cell phone redirection will never lead one to finding other contraband in the same way detection systems can assist.

Fourthly, if a smart phone is jammed or denied service, the phone still can have great utility to the inmate and provide a real and present threat. The inmate can generate or receive pictures, videos, emails, text messages, and other popular phone activities, saving the data to the memory cards which can be easily smuggled in and out of a facility daily. The point being, if a cell phone can find its way to an inmate by whatever path, surely SIM and Memory cards will find their way into the facility by the same routes. Breaking the RF link will create a communications delay for the inmate, the sneaker net vs. the RF link, but the threat is still every bit as real.


One might make the argument that if the phone never transmits, a cell phone detection system will not discover the phone either. While this is correct, to this point a PhD. physiologist with 30 years of corrections experience indicated that it is the nature of man to occasionally try the phone testing the system. When they do the detection system will alert the staff to the presence and location of the phone activity.

Any implementation of a system where the intent is to deny service to cellular traffic, must consider a number of critical issues. These issues are above and beyond non-interference to neighbors adjacent to a correctional facility. There must be a requirement for an automatic system kill switch in the case of a real emergency such as fire or health emergency where first responders. Ideally every facility emergency system should be capable of disabling any Cellular Interruption System (CIS). The CIS must have a remote control kill switch for first responders and not just prison staff, similar to the elevator keys used by fire departments today. The use of cellular based devices whose sole purpose is to communicate vital signs of a patient over the carrier network must be preserved since a patient's life may weigh in the balance. These are but a couple of examples and as the public becomes more and more dependent on cellular technology attaching life critical modalities, so will the complexity of a CIS that operates in the cellular spectra or any public spectrum used for this purpose.

Individual systems offered today do meet all of the functions to address the contraband cell phone threat including detection systems. Systems that transmit can have some have very undesirable and unintended consequences which may prove more a difficult technology challenge to resolve than the initial problem being addressed.

In the meantime the best solution or workable solution may be a combination of technologies integrated to maximize their strengths. Any solution that is truly a solution and not just a masking of the unmonitored communication must enable the security staff the highest probability to capture and remove of the hardware.

Respectfully submitted,

CellSafe LLC.
By: 

Terry L. Bittner – Principle Owner
15201 Frederick Road
Woodbine, MD 21797
443-253-8424

tlbittner@cs.com

July 17, 2013